1xx Informational response

An informational response indicates that the request was received and understood. It is issued on a provisional basis while request processing continues. It alerts the client to wait for a final response. The message consists only of the status line and optional header fields, and is terminated by an empty line. As the HTTP/1.0 standard did not define any 1xx status codes, servers *must not*[note 1] send a 1xx response to an HTTP/1.0 compliant client except under experimental conditions.[3]

100 Continue

The server has received the request headers and the client should proceed to send the request body (in the case of a request for which a body needs to be sent; for example, a POST request). Sending a large request body to a server after a request has been rejected for inappropriate headers would be inefficient. To have a server check the request's headers, a client must send `Expect: 100-continue` as a header in its initial request and receive a `100 Continue` status code in response before sending the body. If the client receives an error code such as 403 (Forbidden) or 405 (Method Not Allowed) then it shouldn't send the request's body. The response `417 Expectation Failed` indicates that the request should be repeated without the `Expect` header as it indicates that the server doesn't support expectations (this is the case, for example, of HTTP/1.0 servers).[4]

101 Switching Protocols

The requester has asked the server to switch protocols and the server has agreed to do so.[5]

102 Processing (WebDAV; RFC 2518)

A WebDAV request may contain many sub-requests involving file operations, requiring a long time to complete the request. This code indicates that the server has received and is processing the request, but no response is available yet.[6] This prevents the client from timing out and assuming the request was lost.

103 Early Hints (RFC 8297)

Used to return some response headers before final HTTP message.[7]

2xx Success

This class of status codes indicates the action requested by the client was received, understood and accepted.[2]

200 OK

Standard response for successful HTTP requests. The actual response will depend on the request method used. In a GET request, the response will contain an entity corresponding to the requested resource. In a POST request, the response will contain an entity describing or containing the result of the action.[8]

201 Created

The request has been fulfilled, resulting in the creation of a new resource.[9]

202 Accepted

The request has been accepted for processing, but the processing has not been completed. The request might or might not be eventually acted upon, and may be disallowed when processing occurs.[10]

203 Non-Authoritative Information (since HTTP/1.1)

The server is a transforming proxy (e.g. a *Web accelerator*) that received a 200 OK from its origin, but is returning a modified version of the origin's response.[11][12]

204 No Content

The server successfully processed the request and is not returning any content.[13]

205 Reset Content

The server successfully processed the request, but is not returning any content. Unlike a 204 response, this response requires that the requester reset the document view.[14]

206 Partial Content (RFC 7233)

The server is delivering only part of the resource (byte serving) due to a range header sent by the client. The range header is used by HTTP clients to enable resuming of interrupted downloads, or split a download into multiple simultaneous streams.[15]

207 Multi-Status (WebDAV; RFC 4918)

The message body that follows is by default an XML message and can contain a number of separate response codes, depending on how many sub-requests were made.[16]

208 Already Reported (WebDAV; RFC 5842)

The members of a DAV binding have already been enumerated in a preceding part of the (multistatus) response, and are not being included again.

226 IM Used (RFC 3229)

The server has fulfilled a request for the resource, and the response is a representation of the result of one or more instance-manipulations applied to the current instance.[17]

3xx Redirection

This class of status code indicates the client must take additional action to complete the request. Many of these status codes are used in URL redirection.[2]

A user agent may carry out the additional action with no user interaction only if the method used in the second request is GET or HEAD. A user agent may automatically redirect a request. A user agent should detect and intervene to prevent cyclical redirects.[18]

300 Multiple Choices

Indicates multiple options for the resource from which the client may choose (via agent-driven content negotiation). For example, this code could be used to present multiple video format options, to list files with different filename extensions, or to suggest word-sense disambiguation.[19]

301 Moved Permanently

This and all future requests should be directed to the given URI.[20]

302 Found (Previously "Moved temporarily")

Tells the client to look at (browse to) another URL. 302 has been superseded by 303 and 307. This is an example of industry practice contradicting the standard. The HTTP/1.0 specification (RFC 1945) required the client to perform a temporary redirect (the original describing phrase was "Moved Temporarily"),[21] but popular browsers implemented 302 with the functionality of a 303 See Other. Therefore, HTTP/1.1 added status codes 303 and 307 to distinguish between the two behaviours.[22] However, some Web applications and frameworks use the 302 status code as if it were the 303.[23]

303 See Other (since HTTP/1.1)

The response to the request can be found under another URI using the GET method. When received in response to a POST (or PUT/DELETE), the client should presume that the server has received the data and should issue a new GET request to the given URI.[24]

304 Not Modified (RFC 7232)

Indicates that the resource has not been modified since the version specified by the request headers If-Modified-Since or If-None-Match. In such case, there is no need to retransmit the resource since the client still has a previously-downloaded copy.[25]

305 Use Proxy (since HTTP/1.1)

The requested resource is available only through a proxy, the address for which is provided in the response. For security reasons, many HTTP clients (such as Mozilla Firefox and Internet Explorer) do not obey this status code.[26]

306 Switch Proxy

No longer used. Originally meant "Subsequent requests should use the specified proxy."[27]

307 Temporary Redirect (since HTTP/1.1)

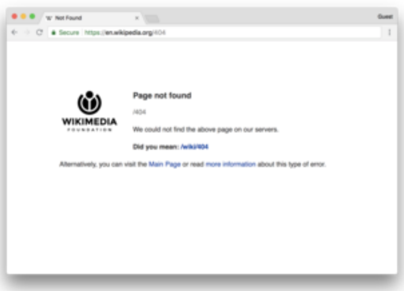
In this case, the request should be repeated with another URI; however, future requests should still use the original URI. In contrast to how 302 was historically implemented, the request method is not allowed to be changed when reissuing the original request. For example, a POST request should be repeated using another POST request.[28]

308 Permanent Redirect (RFC 7538)

The request and all future requests should be repeated using another URI. 307 and 308 parallel the behaviors of 302 and 301, but *do not allow the HTTP method to change*. So, for example, submitting a form to a permanently redirected resource may continue smoothly.[29]

4xx Client errors

This class of status code is intended for situations in which the error seems to have been caused by the client. Except when responding to a HEAD request, the server *should* include an entity containing an explanation of the error situation, and whether it is a temporary or permanent condition. These status codes are applicable to any request method. User agents *should* display any included entity to the user.[30]



Page not found

/404

We could not find the above page on our servers.

Did you mean: /wiki/404

Alternatively, you can visit the Main Page or read more information about this type of error.

404 error on Wikipedia

400 Bad Request

The server cannot or will not process the request due to an apparent client error (e.g., malformed request syntax, size too large, invalid request message framing, or deceptive request routing).[31]

401 Unauthorized (RFC 7235)

Similar to *403 Forbidden*, but specifically for use when authentication is required and has failed or has not yet been provided. The response must include a WWW-Authenticate header field containing a challenge applicable to the requested resource. See Basic access authentication and Digest access authentication.[32] 401 semantically means "unauthorised",[33] the user does not have valid authentication credentials for the target resource.

Note: Some sites incorrectly issue HTTP 401 when an IP address is banned from the website (usually the website domain) and that specific address is refused permission to access a website.

402 Payment Required

Reserved for future use. The original intention was that this code might be used as part of some form of digital cash or micropayment scheme, as proposed, for example, by GNU Taler,[34] but that has not yet happened, and this code is not usually used. Google Developers API uses this status if a particular developer has exceeded the daily limit on requests.[35] Sipgate uses this code if an account does not have sufficient funds to start a call.[36] Shopify uses this code when the store has not paid their fees and is temporarily disabled.[37] Stripe uses this code for failed payments where parameters were correct, for example blocked fraudulent payments.[38]

403 Forbidden

The request contained valid data and was understood by the server, but the server is refusing action. This may be due to the user not having the necessary permissions for a resource or needing an account of some sort, or attempting a prohibited action (e.g. creating a duplicate record where only one is allowed). This code is also typically used if the request provided authentication via the WWW-Authenticate header field, but the server did not accept that authentication. The request should not be repeated.

404 Not Found

The requested resource could not be found but may be available in the future. Subsequent requests by the client are permissible.

405 Method Not Allowed

A request method is not supported for the requested resource; for example, a GET request on a form that requires data to be presented via POST, or a PUT request on a read-only resource.

406 Not Acceptable

The requested resource is capable of generating only content not acceptable according to the Accept headers sent in the request.[39] See Content negotiation.

407 Proxy Authentication Required (RFC 7235)

The client must first authenticate itself with the proxy.[40]

408 Request Timeout

The server timed out waiting for the request. According to HTTP specifications: "The client did not produce a request within the time that the server was prepared to wait. The client MAY repeat the request without modifications at any later time."[41]

409 Conflict

Indicates that the request could not be processed because of conflict in the current state of the resource, such as an edit conflict between multiple simultaneous updates.

410 Gone

Indicates that the resource requested is no longer available and will not be available again. This should be used when a resource has been intentionally removed and the resource should be purged. Upon receiving a 410 status code, the client should not request the resource in the future. Clients such as search engines should remove the resource from their indices.[42] Most use cases do not require clients and search engines to purge the resource, and a "404 Not Found" may be used instead.

411 Length Required

The request did not specify the length of its content, which is required by the requested resource.[43]

412 Precondition Failed (RFC 7232)

The server does not meet one of the preconditions that the requester put on the request header fields.[44][45]

413 Payload Too Large (RFC 7231)

The request is larger than the server is willing or able to process. Previously called "Request Entity Too Large".[46]

414 URI Too Long (RFC 7231)

The URI provided was too long for the server to process. Often the result of too much data being encoded as a query-string of a GET request, in which case it should be converted to a POST request.[47] Called "Request-URI Too Long" previously.[48]

415 Unsupported Media Type (RFC 7231)

The request entity has a media type which the server or resource does not support. For example, the client uploads an image as image/svg+xml, but the server requires that images use a different format.[49]

416 Range Not Satisfiable (RFC 7233)

The client has asked for a portion of the file (byte serving), but the server cannot supply that portion. For example, if the client asked for a part of the file that lies beyond the end of the file.[50] Called "Requested Range Not Satisfiable" previously.[51]

417 Expectation Failed

The server cannot meet the requirements of the Expect request-header field.[52]

418 I'm a teapot (RFC 2324, RFC 7168)

This code was defined in 1998 as one of the traditional IETF April Fools' jokes, in RFC 2324, *Hyper Text Coffee Pot Control Protocol*, and is not expected to be implemented by actual HTTP servers. The RFC specifies this code should be returned by teapots requested to brew coffee.[53] This HTTP status is used as an Easter egg in some websites, including Google.com.[54][55]

421 Misdirected Request (RFC 7540)

The request was directed at a server that is not able to produce a response[56] (for example because of connection reuse).[57]

422 Unprocessable Entity (WebDAV; RFC 4918)

The request was well-formed but was unable to be followed due to semantic errors.[16]

423 Locked (WebDAV; RFC 4918)

The resource that is being accessed is locked.[16]

424 Failed Dependency (WebDAV; RFC 4918)

The request failed because it depended on another request and that request failed (e.g., a PROPPATCH).[16]

425 Too Early (RFC 8470)

Indicates that the server is unwilling to risk processing a request that might be replayed.

426 Upgrade Required

The client should switch to a different protocol such as TLS/1.0, given in the Upgrade header field.[58]

428 Precondition Required (RFC 6585)

The origin server requires the request to be conditional. Intended to prevent the 'lost update' problem, where a client GETs a resource's state, modifies it, and PUTs it back to the server, when meanwhile a third party has modified the state on the server, leading to a conflict.[59]

429 Too Many Requests (RFC 6585)

The user has sent too many requests in a given amount of time. Intended for use with rate-limiting schemes.[59]

431 Request Header Fields Too Large (RFC 6585)

The server is unwilling to process the request because either an individual header field, or all the header fields collectively, are too large.[59]

451 Unavailable For Legal Reasons (RFC 7725)

A server operator has received a legal demand to deny access to a resource or to a set of resources that includes the requested resource.[60] The code 451 was chosen as a reference to the novel *Fahrenheit 451* (see the Acknowledgements in the RFC).

5xx Server errors

The server failed to fulfill a request.[61]

Response status codes beginning with the digit "5" indicate cases in which the server is aware that it has encountered an error or is otherwise incapable of performing the request. Except when responding to a HEAD request, the server *should* include an entity containing an explanation of the error situation, and indicate whether it is a temporary or permanent condition. Likewise, user agents *should* display any included entity to the user. These response codes are applicable to any request method.[62]

500 Internal Server Error

A generic error message, given when an unexpected condition was encountered and no more specific message is suitable.[63]

501 Not Implemented

The server either does not recognize the request method, or it lacks the ability to fulfil the request. Usually this implies future availability (e.g., a new feature of a web-service API).[64]

502 Bad Gateway

The server was acting as a gateway or proxy and received an invalid response from the upstream server.[65]

503 Service Unavailable

The server cannot handle the request (because it is overloaded or down for maintenance). Generally, this is a temporary state.[66]

504 Gateway Timeout

The server was acting as a gateway or proxy and did not receive a timely response from the upstream server.[67]

505 HTTP Version Not Supported

The server does not support the HTTP protocol version used in the request.[68]

506 Variant Also Negotiates (RFC 2295)

Transparent content negotiation for the request results in a circular reference.[69]

507 Insufficient Storage (WebDAV; RFC 4918)

The server is unable to store the representation needed to complete the request.[16]

508 Loop Detected (WebDAV; RFC 5842)

The server detected an infinite loop while processing the request (sent instead of 208 Already Reported).

510 Not Extended (RFC 2774)
: Further extensions to the request are required for the server to fulfil it.[70]

511 Network Authentication Required (RFC 6585)
: The client needs to authenticate to gain network access. Intended for use by intercepting proxies used to control access to the network (e.g., "captive portals" used to require agreement to Terms of Service before granting full Internet access via a Wi-Fi hotspot).[59]

Unofficial codes

The following codes are not specified by any standard.

103 Checkpoint
: Used in the resumable requests proposal to resume aborted PUT or POST requests.[71]

218 This is fine (Apache Web Server)
: Used as a catch-all error condition for allowing response bodies to flow through Apache when ProxyErrorOverride is enabled. When ProxyErrorOverride is enabled in Apache, response bodies that contain a status code of 4xx or 5xx are automatically discarded by Apache in favor of a generic response or a custom response specified by the ErrorDocument directive.[72]

419 Page Expired (Laravel Framework)
: Used by the Laravel Framework when a CSRF Token is missing or expired.

420 Method Failure (Spring Framework)
: A deprecated response used by the Spring Framework when a method has failed.[73]

420 Enhance Your Calm (Twitter)
: Returned by version 1 of the Twitter Search and Trends API when the client is being rate limited; versions 1.1 and later use the 429 Too Many Requests response code instead.[74]

430 Request Header Fields Too Large (Shopify)
: Used by Shopify, instead of the 429 Too Many Requests response code, when too many URLs are requested within a certain time frame.[75]

450 Blocked by Windows Parental Controls (Microsoft)
: The Microsoft extension code indicated when Windows Parental Controls are turned on and are blocking access to the requested webpage.[76]

498 Invalid Token (Esri)
: Returned by ArcGIS for Server. Code 498 indicates an expired or otherwise invalid token.[77]

499 Token Required (Esri)
: Returned by ArcGIS for Server. Code 499 indicates that a token is required but was not submitted.[77]

509 Bandwidth Limit Exceeded (Apache Web Server/cPanel)
: The server has exceeded the bandwidth specified by the server administrator; this is often used by shared hosting providers to limit the bandwidth of customers.[78]

526 Invalid SSL Certificate
: Used by Cloudflare and Cloud Foundry's gorouter to indicate failure to validate the SSL/TLS certificate that the origin server presented.

529 Site is overloaded
: Used by Qualys in the SSLLabs server testing API to signal that the site can't process the request.[79]

530 Site is frozen
: Used by the Pantheon web platform to indicate a site that has been frozen due to inactivity.[80]

598 (Informal convention) Network read timeout error
: Used by some HTTP proxies to signal a network read timeout behind the proxy to a client in front of the proxy.[81]

Internet Information Services

Microsoft's Internet Information Services (IIS) web server expands the 4xx error space to signal errors with the client's request.

440 Login Time-out
: The client's session has expired and must log in again.[82]

449 Retry With
: The server cannot honour the request because the user has not provided the required information.[83]

451 Redirect
: Used in Exchange ActiveSync when either a more efficient server is available or the server cannot access the users' mailbox.[84] The client is expected to re-run the HTTP AutoDiscover operation to find a more appropriate server.[85]

IIS sometimes uses additional decimal sub-codes for more specific information,[86] however these sub-codes only appear in the response payload and in documentation, not in the place of an actual HTTP status code.

nginx

The nginx web server software expands the 4xx error space to signal issues with the client's request.[87][88]

444 No Response

Used internally[89] to instruct the server to return no information to the client and close the connection immediately.

494 Request header too large

Client sent too large request or too long header line.

495 SSL Certificate Error

An expansion of the 400 Bad Request response code, used when the client has provided an invalid client certificate.

496 SSL Certificate Required

An expansion of the 400 Bad Request response code, used when a client certificate is required but not provided.

497 HTTP Request Sent to HTTPS Port

An expansion of the 400 Bad Request response code, used when the client has made a HTTP request to a port listening for HTTPS requests.

499 Client Closed Request

Used when the client has closed the request before the server could send a response.

Cloudflare

Cloudflare's reverse proxy service expands the 5xx series of errors space to signal issues with the origin server.[90]

520 Web Server Returned an Unknown Error

The origin server returned an empty, unknown, or unexplained response to Cloudflare.[91]

521 Web Server Is Down

The origin server has refused the connection from Cloudflare.

522 Connection Timed Out

Cloudflare could not negotiate a TCP handshake with the origin server.

523 Origin Is Unreachable

Cloudflare could not reach the origin server; for example, if the DNS records for the origin server are incorrect.

524 A Timeout Occurred

Cloudflare was able to complete a TCP connection to the origin server, but did not receive a timely HTTP response.

525 SSL Handshake Failed

Cloudflare could not negotiate a SSL/TLS handshake with the origin server.

526 Invalid SSL Certificate

Cloudflare could not validate the SSL certificate on the origin web server.

527 Railgun Error

Error 527 indicates an interrupted connection between Cloudflare and the origin server's Railgun server.[92]